SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

Controlling Access to Data Stored on a Storage Device of a Trusted Computing Platform System

Cross Reference to Related Applications

The interested reader is referred, for assistance in understanding the inventions here described to U.S. Patents 5,388,156, issued February 7, 1995, and 6229,712, issued May 8, 2001, both held in common with inventions here described. The referenced patents are relevant to the description which follows and are hereby incorporated by reference into this description as fully as if here repeated in full. Specific references to portions of the prior patents to which attention is directed follow an effort toward brevity of the description here given.

Background of Invention

[0001] Personal computer systems as described and shown, for example, in U.S. Pat. 5,388,156 beginning in Column 6 at line 33 and continuing through Column 8 at line 19 and related Figures 1 through 3 have been known and in use for some time. Configurations for such systems can vary from those shown in the "156 patent disclosure here incorporated by reference, as is known to persons of skill in the applicable arts and illustrated by other patent disclosures including the "712 patent disclosure beginning in Column 2 at line 24 and related Figures 1 through 3, The patents here referenced have been selected merely as being exemplary and due to ownership in common with the inventions here disclosed.

[0002]

Concern over the security and authenticity of transactions through and over computer systems has become a growing concern as the use of computer systems has proliferated. That concern has given rise to the Trusted Computing Platform Alliance,

also know as the TCPA. The Design Philosophies statement of the TCPA states that the purpose of the activity is to encourage the use of computer platforms for critical purposes by improving the basis on which a computing environment may be trusted.

[0003] The TCPA has developed a specification in addition to the Design Philosophy statement, and included in their materials a glossary of terminology used in their discussions. Certain terms appearing hereinafter may be found in that glossary as well as having meaning apart from the glossary definitions offered by the TCPA. While it is intended that the glossary definitions will be helpful, it is to be recognized at the outset of the discussion which follows that those definitions are deemed illustrative only and not fully binding on the terminology used. The choice of TCPA defined terms is made only for convenience and as an aid to understanding, avoiding restriction to those definitions as the meaning of the terminology is expected to expand as the technology becomes into wider use.

[0004] A Trusted Computing Platform (TCP) is a platform that can be trusted by local users and by remote entities. TCPA uses a behavioral definition of trust: an entity can be trusted if it always behaves in the expected manner for the intended purpose. The basis for trusting a platform, or computer system, is a declaration by a known authority that a platform with a given identity can be trusted to measure and report the way it is operating.

[0005] As evidenced by the TCPA and the referenced prior "156 patent, there have been concerns over the security of information stored in such computer systems, and steps have been taken to enable protection of such information. Conventionally, such protection is left to the selection and implementation of a system owner or a designated administrator for the system owner. In some instances, choices are made that information protection will not be enabled. In other instances, choices are made that information protection will be maximized.

[0006] In the latter instance, where protection of information is to be maximized, recognition can be given to the fact that a read/write storage device may be exchanged from one computer system to another computer system. Where the read/write storage device is the somewhat traditional rotating disk, magnetic media device known as a hard drive or hard file, that exchange may be more or less difficult,

depending upon the manner in which the system is housed. With a conventional system of the type known as a desktop workstation, exchange of a storage device may require significant dismantling of the system. With certain notebook systems, the exchange is relatively quick and easy. With devices which are intentionally detachable, such as a device coupled through a Universal Serial Bus (USB) port, the exchange is trivial. Indeed, with the last mentioned class of storage devices, the very triviality of exchange is touted as an advantage, enabling ready mobility of data files. The last mentioned class of devices, as currently available, include flash and DRAM memory arrays, as well as rotating disc magnetic and optical media.

[0007] One existing approach to the security problems presented by such portability is the provision of a password specifically associated with the storage device. As an example only, a hard disk supplied with a notebook system usually has the capability of setting what may be known as a hard drive password. Thus there may be password protection for access to the boot capability, and separate password protection for access to the storage device. If a storage device password is correctly passed to the storage device or hacked, then full access to the contents of the device is enabled. For certain purposes, the level of security thus attained may still be below what may be optimal.

[0008] A prior related invention addressed certain such issues and is described in an application filed 13 May 2002 under the title Secure Control of Access to Data Stored on a Storage Device of a Computer System and having certain named inventors in common with the inventions here described. To any extent necessary to a full understanding of this invention, that prior application is here incorporated by reference. The distinctions between the inventions of the two applications will become more clear from the discussion which follows.

Summary of Invention

[0009] The present invention deems it desirable to employ the capabilities of a computer system which has characteristics of a Trusted Computing Platform to provide enhanced security controlling access to data files stored in a read/write storage device of the types described above. In pursuing this goal, the present invention contemplates that a storage device may be specifically linked to a specific computer

system, and linked in such a way that access will be granted only when a series of exchanges exemplary of that linkage and of the implementation of Trusted Computing Platform technology occurs.

[0010] Stated differently, the present invention contemplates that access to data stored in a read/write storage device is to be granted only when the device is associated with a specific computer system and further only when appropriate password entry is verified in accordance with procedures compatible with the characteristics of a TCP.

Brief Description of Drawings

[0011] Some of the purposes of the invention having been stated, others will appear as the description proceeds, when taken in connection with the accompanying drawings, in which:

[0012] Figure 1 is a representation of a sequence of steps followed on initial linking of a storage device to a computer system;

[0013] Figure 2 is a representation of a sequence of steps followed when a computer system having a storage device linked through an operation such as that of Figure 1 is subsequently brought into operation;

[0014] Figure 3 is a representation of certain components of a computer systems with trusted computing platform capabilities; and

[0015] Figure 4 is a representation of a computer readable medium carrying instructions effective to cause the sequences of Figures 1 and 2 in a system such as represented in Figure 3.

Detailed Description

[0016]

While the present invention will be described more fully hereinafter with reference to the accompanying drawings, in which a preferred embodiment of the present invention is shown, it is to be understood at the outset of the description which follows that persons of skill in the appropriate arts may modify the invention here described while still achieving the favorable results of the invention. Accordingly, the description which follows is to be understood as being a broad, teaching disclosure

directed to persons of skill in the appropriate arts, and not as limiting upon the present invention.

[0017] Briefly stated, the present invention encompasses a method of operating a computer system during installation of a storage device to be protected, a method of operating the system during subsequent access to the storage device, a computer system configured for such access control, and the provision of program instructions enabling controls as here described.

[0018] Specific illustrations of a computer system and certain elements of the system are here omitted, reliance being placed on the incorporations by reference set forth above. For purposes of the present discussion, it is contemplated by the present invention that the computer system implementing this invention have an accessible read/write storage device and Trusted Computing Platform capabilities. In that regard, the system contemplated here differs in some detail from those illustrated in the previously mentioned prior patents. Most usually, the storage device will be a magnetic media, rotating disk device of the type known as a hard drive and will be included within a common housing with other components of the system. However, it is known that the storage device may be optically based, or be based on a type of memory known as flash memory, and may be accessed through a USB or network connection rather than being directly housed within a common enclosure with the other components of the system. One example is illustrated at 19 in Figure 3 of the "712 referenced patent.

[0019] The present invention contemplates that a read/write storage device may be identified or bound to a specific computer system by the creation of what is here called a binding key on initial installation of the storage device. In so binding the system and device, a sequence is followed in which a drive to be installed in a system is initialized by the creation of first random number key, herein also called a salt key, which is stored in a secure area of the drive. Thereafter, program instructions effective on powering on of the system to initiate system operation, typically known and referenced as BIOS code (see the discussion in the "156 patent) identify the presence of the read/write storage device and reads an endorsement public key from a Trusted Platform Module (TPM) provided in the system and stores that key in a read only area

of the drive (see materials from the Trusted Computing Platform Alliance mentioned above). The BIOS also prompts a user of the system to enter a password for controlling access to the read/write storage device, generates a hash value from the password and stores that hash value in the storage device. The system then generates a hash value from the first random number key and the password and stores the first key/password hash value in a protected area of the read/write storage device for subsequent retrieval in exercising control of system access to the read/write storage device. These steps are illustrated in Figure 1.

[0020] The generation of a hash value is a known technique in which an otherwise meaningless value is created by applying a known algorithm to a data string or set. One usual purpose of hashing, exercised here, is to reduce the length or size of a data record, in order that less storage space be required or less time be expended in transferring the value.

[0021] The storage of the password hash value and first key/password hash value in the storage device enables a particular sequence when the device is later to be accessed as for use. When the system is powered on in anticipation of a work session, the BIOS code executes to initiate system operation. In response to powering on, a nonce string is generated in the read/write storage device. As here used, the word nonce indicates a one time, non-recurring, event. That is, nonce is used in the dictionary sense of the present or immediate occasion or purpose. This generation of a nonce string is a significant feature of the security obtained, as will be pointed out hereinafter. On each subsequent powering on of the system, the string generated as the nonce string differs from whatever may have been previously, or will next subsequently be, generated. A nonce string is used in the previously mentioned co-pending application.

[0022] In the invention to which this description is directed, the nonce string is read by the BIOS and extended into a Platform Configuration Register (PCR), the presence of which is characteristic of a TCP.

[0023] The BIOS code may distinguish between a requirement for entry of at least one password to access the read/write storage device and no requirement for entry of a password, which is a normal BIOS function. In response to a requirement for password

entry, an operator is prompted to enter a password by determination that entry of a password is required to access the read/write storage device. When the password is supplied, the code extends the password into the same PCR to which the nonce string has been extended. The BIOS then quotes the PCR, with the quoted output being a signed value, signed with the endorsement key of the TPM included in the system. The quote is sent to the storage device, where it is verified against the TPM endorsement public key earlier stored. If verified correct, then read/write access to the read/write storage device is granted. These steps are illustrated in Figure 2.

[0024] Inclusion of the nonce string in these sequences protects against capture of the hash value in an effort to hack the security of the storage device. Further, inclusion of the TPM keys protects against the possibility of hacking access to the storage device from a system other than the one to which is it specifically bound. Use of hash values minimizes the storage space required to make the invention operative.

[0025] In use, an apparatus which implements these procedures will have a computer system with TCP capabilities, a read/write storage device accessible to the system in the manners described above, and a keys as described stored accessibly to said system and said storage device and identifying the system and storage device as being specifically linked. Additionally, the apparatus will have program instructions such as BIOS code stored accessibly to the system and storage device and operative when executing on the system and storage device to generate a nonce string as here defined in the read/write storage device in response to powering on of the system and prompt an operator of the system to enter a password associated with access to the storage device. The system will, in executing the instructions, extend the nonce string and the password into a platform configuration register, then quote the register contests as a signed value (confirming with the TPM key). The storage device will act to verify that the quote is derived from the nonce string, the password and the TPM endorsement key and grant read/write access to the read/write storage device on verification. Such an apparatus may be as illustrated in Figures 1 through 3 of each of the "156 and "712 patents referenced above, with exceptions now to be addressed.

[0026] In particular, Figure 3 is an illustration drawn from the TCPA PC Specific Implementation Specification to illustrate the presence of certain elements of the

system. Most significantly, the system has a trusted platform module 31which enables TCP functionality including an endorsement public key and an endorsement private key used as mentioned above.

[0027] Figure 4 illustrates a computer readable medium in the form of a diskette 10 bearing program instructions readable by a system such as that of Figure 3 and effective on execution by such a system to perform the steps of Figures 1 and 2 of this description.

[0028] In the drawings and specifications there has been set forth a preferred embodiment of the invention and, although specific terms are used, the description thus given uses terminology in a generic and descriptive sense only and not for purposes of limitation.